

**AMENDMENTS TO THE CLAIMS**

This listing of claims will replace all prior versions, and listings, of claims in the application:

**Listing of Claims:**

1. (Currently Amended): An apparatus for session control in a wireless communication network, comprising:  
a stateful inspector configured to detect ~~[means for detecting]~~ requested application-specific packets in a packet stream ~~[; means for blocking]~~ and configured to block application-specific packets in the packet stream that are not the requested application-specific packets; and  
a session manager configured to activate ~~[means for activating]~~, in response to the stateful inspector ~~[means for]~~ detecting the requested application-specific packets, a plurality of packet sessions with application-specific QoS parameters, without requiring explicit cooperation of application software.
2. (Currently Amended): The apparatus of claim 1 ~~[further comprising means for deactivating]~~ wherein the session manager is further configured to deactivate at least one of the plurality of packet sessions.
3. (Previously presented): The apparatus of claim 1 wherein the wireless communication network comprises a UMTS radio access network.
4. (Currently Amended): The apparatus of claim 1, wherein the plurality of packet sessions ~~[comprise]~~ comprises Packet Data Protocol (PDP) contexts.

5. (Currently Amended): The apparatus of claim 1 [~~wherein the means for detecting comprises stateful inspection means, and the apparatus~~] further [~~comprises session manager means and~~] comprising a packet filter [~~means~~] responsive to the stateful inspector [~~inspection means~~].
6. (Currently Amended): The apparatus of claim 1, wherein the stateful inspector [~~means for detecting~~] is [~~arranged~~] configured to inspect uplink packet flows to detect application-specific packet flows, via application-specific control messages.
7. (Currently Amended): The apparatus of claim 1, wherein the stateful inspector [~~means for detecting~~] is [~~arranged~~] configured to inspect downlink packet flows to detect application-specific packet flows, via application-specific control messages.
8. (Currently Amended): The apparatus of claim 1, wherein the plurality of packet sessions [~~comprise~~] comprises conversational class PDP contexts.
9. (Previously presented): The apparatus of claim 8, wherein the conversational class PDP contexts are arranged to carry Voice over IP (VOIP) traffic.
10. (Currently Amended): The [~~arrangement~~] apparatus of claim 8, wherein the conversational class PDP contexts are arranged to carry Video over IP traffic.
11. (Previously presented): The apparatus of claim 9 wherein the traffic is based on originated calls controlled by Session Initiation Protocol (SIP).
12. (Previously presented): The apparatus of claim 9 wherein the traffic is based on originated calls controlled by H.323 protocol.

13. (Currently Amended): The apparatus of claim 1, wherein the plurality of packet sessions [~~comprise~~] comprises streaming class PDP contexts.

14. (Previously Presented): The apparatus of claim 13, wherein the streaming class PDP contexts are arranged to carry streaming media traffic controlled by Real Time Streaming Protocol.

15. (Currently Amended): The apparatus of claim 1, wherein the plurality of packet sessions [~~comprise~~] comprises interactive class PDP contexts.

16. (Currently Amended): The apparatus of claim 1, wherein the plurality of packet sessions comprise background class PDP contexts.

17. (Previously presented): The apparatus of claim 16, wherein the background class PDP contexts are arranged to carry Post Office Protocol-Version 3 (POP3) traffic.

18. (Previously presented): The apparatus of claim 16, wherein the background class PDP contexts are arranged to carry Simple Mail Transfer Protocol (SMTP) traffic.

19. (Previously presented): A method for session control in a wireless communication network, comprising:

detecting requested application-specific packets in a packet stream;

blocking application-specific packets in the packet stream that are not the requested application-specific packets; and

activating, in response to detecting the requested application-specific packets, a plurality of packet sessions with application-specific QoS parameters, without requiring explicit cooperation of application software.

20. (Original): The method of claim 19 further comprising deactivating at least one of the plurality of packet sessions.
21. (Previously presented): The method of claim 19 wherein the wireless communication network comprises a UMTS radio access network.
22. (Currently Amended): The method of claim 19, wherein the plurality of packet sessions [~~comprise~~] comprises Packet Data Protocol (PDP) contexts.
23. (Currently Amended): The method of claim 19, wherein detecting comprises detecting in a stateful inspector, and the method further comprises providing a session manager and a packet filter responsive to the stateful inspector [~~inspection means~~].
24. (Previously presented): The method of claim 19, wherein detecting comprises inspecting uplink packet flows to detect application-specific packet flows, via application-specific control messages.
25. (Previously presented): The method of claim 19, wherein detecting comprises inspecting downlink packet flows to detect application-specific packet flows, via application-specific control messages.
26. (Currently Amended): The method of claim 19, wherein the plurality of packet sessions [~~comprise~~] comprises conversational class PDP contexts.
27. (Original): The method of claim 26, wherein the conversational class PDP contexts carry Voice over IP (VOIP) traffic.

28. (Original): The method of claim 26, wherein the conversational class PDP contexts carry Video over IP traffic.

29. (Previously presented): The method of claim 27 wherein the traffic is based on originated calls controlled by Session Initiation Protocol (SIP).

30. (Previously presented): The method of claim 27 wherein the traffic is based on originated calls controlled by H.323 protocol.

31. (Currently Amended): The method of claim 19, wherein the plurality of packet sessions [~~comprise~~] comprises streaming class PDP contexts.

32. (Original): The method of claim 31, wherein the streaming class PDP contexts carry streaming media traffic controlled by Real Time Streaming Protocol.

33. (Currently Amended): The method of claim 19, wherein the plurality of packet sessions [~~comprise~~] comprises interactive class PDP contexts.

34. (Currently Amended): The method of claim 19, wherein the plurality of packet sessions [~~comprise~~] comprises background class PDP contexts.

35. (Original): The method of claim 34, wherein the background class PDP contexts carry Post Office Protocol-Version 3 (POP3) traffic.

36. (Original): The method of claim 34, wherein the background class PDP contexts carry Simple Mail Transfer Protocol (SMTP) traffic.

37. (Previously presented): The method of claim 19, wherein the method is performed in User equipment (UE).
38. (Previously presented): User equipment (UE) for use in a UTRA system, the user equipment comprising the apparatus of claim 1.
39. (Previously presented): An integrated circuit comprising the apparatus of claim 1.
40. (Currently Amended): A non-transitory computer program element having executable program code stored therein ~~[program code]~~ for session control in a wireless communication network, the program code operable for [serving to] when executed at a user equipment:  
detecting [detect] requested application-specific packets in a packet stream;  
blocking [block] application-specific packets in the packet stream that are not the requested application-specific packets; and  
activating [activate], in response to detecting the requested application-specific packets, a plurality of packet sessions with application-specific QoS parameters, without requiring explicit cooperation of application software.
41. (Currently Amended): The apparatus of claim 1 [5], wherein ~~[detecting in a]~~ the stateful inspector is configured to inspect ~~[comprises inspecting]~~ packets, implying a state of an application-specific packet session via inspected control packets and allowing packets for a [said] session to flow through a [the] firewall if said session originated from inside the firewall or otherwise, blocking said session ~~[otherwise]~~.
42. (Currently Amended): The method of claim 23, wherein detecting in a stateful inspector comprises inspecting packets, implying a state of an application-specific packet session via inspected control packets and allowing packets for a [said] session to flow

through a ~~the~~ firewall if said session originated from inside the firewall or otherwise,  
blocking said session ~~otherwise~~.

43-74. (Canceled).